

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-195383
 (43)Date of publication of application : 15.07.1992

(51)Int.Cl.

G06K 19/073
 B42D 15/10

(21)Application number : 02-328713

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.11.1990

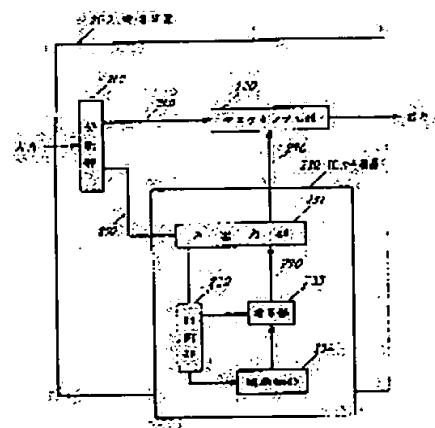
(72)Inventor : MUTO YOSHIHIRO
 TAKAGI SHINYA

(54) IC CARD DEVICE AND RECEIVER USING THE SAME

(57)Abstract:

PURPOSE: To completely protect secret information by providing a RAM for storing the secret information and an auxiliary power source for the RAM in the IC card device and further providing a means which stops supplying electric power to said RAM when an illegal action is taken.

CONSTITUTION: The receiver 200 uses the IC card device 230 and broadcast data are divided by a division part 210 into secret data 250 and sent data 260. The secret data 250 is sent the IC card device 230 with a key parameter. A control part 232 deciphers a key parameter for descrambling the sent data 260 by using the key parameter and the master key of a key storage part 234. A descrambling part descrambles the sent data 260 with the key parameters 270 and outputted the resulting data finally. The RAM stored with the secret information for key deciphering and the power source are connected by a lead line laid around in the IC card device 100 and when this RAM is taken out, the lead wire is broken.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

⑫ 公開特許公報(A) 平4-195383

⑤ Int.Cl.⁵

識別記号

庁内整理番号

④ 公開 平成4年(1992)7月15日

G 06 K 19/073
B 42 D 15/10

5 2 1

9111-2C
6711-5L

G 06 K 19/00

P

審査請求 未請求 請求項の数 2 (全5頁)

⑥ 発明の名称 ICカード装置およびそれを用いた受信装置

⑦ 特 願 平2-328713

⑧ 出 願 平2(1990)11月27日

⑨ 発 明 者	武 藤 義 弘	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑩ 発 明 者	高 木 伸 哉	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑪ 出 願 人	松下電器産業株式会社	大阪府門真市大字門真1006番地	
⑫ 代 理 人	弁理士 小 鍛 治 明	外 2 名	

明 細 書

1. 発明の名称

ICカード装置およびそれを用いた受信装置

2. 特許請求の範囲

(1) CPUと、外部からのコマンドに従った処理を行うためのプログラムを格納するROMと、機密情報を格納するRAMと、前記RAM内のデータを保持するための電源を供給する補助電源と、不正行為が行われた場合に前記RAMへの電源の供給を停止する電源供給遮断手段とを有することを特徴とするICカード装置。

(2) 請求項1に記載のICカード装置が接続された受信装置であって、受信したデータを機密データと通信相手に伝達すべき所望の伝送データとに分割するデータ分割部と、前記機密データから解読鍵を生成する復号部と、前記復号部を作動させるためのマスター鍵を格納している鍵格納部と、生成された前記解読鍵を用いて前記伝送データをデスクランブルするデスクランブル部とから構成され、少なくとも前記鍵格納部が前記ICカ

ード装置上に存在することを特徴とする受信装置

3. 発明の詳細な説明

産業上の利用分野

本発明は、ICカード装置に関するもの、および衛星放送、ケーブルテレビなどの通信において、暗号化された通信データを一定のアルゴリズムに従ってデスクランブルする事の許可をICカード装置によって与える受信装置に関するものである。

従来の技術

放送受信方式において、受信者を限定した通信を行うために、契約時にICカード装置内のROMあるいは書換え可能な不揮発性メモリ(以下EEPROMと呼ぶ)に秘密情報を格納して発行し、ICカード装置を所持している人にのみ受信を許可し、許可されていないもの(具体的には料金未納のもの等)の受信を不可能にしている。

第3図にICカード装置を用いた従来技術の放送受信方式(特開昭62-180625号公報)の基本構成を示す。この放送受信方式はアナログ放送を基本としている。この放送受信方式におい

て、ICカード装置330は受信装置300から復調されデジタル化された信号を入力データとし、入出力部331を通してデスクランブラ則320にデータに引き渡す。デスクランブラ則320は放送センター等に管理されており、予め秘密のプログラムとしてICカード装置330内の書換え可能なメモリに格納されている。デスクランブラ則320はカウンタあるいはタイマ等を利用した制御部332によって制御されている。デスクランブルされたデータは再び入出力部331を通して受信装置300に出力される。このようにデータを復元するデスクランブラ則がICカード装置内に格納され、ICカード装置を所持している人によりのみ放送の受信を許可することを特徴としていた。

発明が解決しようとする課題

デスクランブラ則を長時間変えないでよく、信号の性質を解析するなどの方法でデスクランブラ則が知られてしまう可能性があり、また、従来技術のICカード装置では画像データなどの大量

のデータをデスクランブルするのが困難である。

また、ICカード装置のROMあるいはEEPROM内のデータの安全性が問題となる場合、すなわち技術の進歩によりメモリ内のデータの読み出しが可能となった場合、前記従来の技術で示したICカード装置は必ずしも安全な媒体とはならない。

本発明はかかる点に鑑み、ICカード装置内の機密情報を完全に保護し、このICカード装置を用いた簡単な構成のデータ受信装置を提供することを目的とする。

課題を解決するための手段

本発明は上記目的を達成するために、プログラムに従って命令を実行するCPUと、外部からのコマンドに従った処理を行うためのプログラムを格納するROMと、機密情報を格納するRAMと、前記RAM内のデータを保持するための電源を供給する補助電源と、不正行為が行われた場合に前記RAMへの電源の供給を停止する電源供給遮断手段とを有するICカード装置である。

またこのICカード装置が接続された受信装置であって、受信したデータを機密データと通信相手に伝達すべき所望の伝送データとに分割するデータ分割部と、前記機密データから解読鍵を生成する復号部と、前記復号部を作動させるためのマスター鍵を格納している鍵格納部と、生成された解読鍵を用いて前記伝送データをデスクランブルするデスクランブル部とから構成され、少なくとも前記鍵格納部が前記ICカード装置上に存在することを特徴とする受信装置である。

作用

上記した構成により、このICカード装置に暗号解読や複製を作成することを目的として、分解をしようとした場合には、電源供給遮断手段が作動してRAMへの電源供給を断ち、RAM内に記憶している機密情報を消滅させる。

また、このICカード装置を接続した受信装置においては、デスクランブラ則はICカード装置内には持たず、受信装置本体側に持たせ、ICカード装置にはデスクランブルするためのパラメー

タを復号する機能を設けたのみであり、簡略化される。

そして、このICカード装置は、受信装置本体と自在に接続及び切り離しが行え、このICカード装置を切り離すと受信またはデスクランブルが行うことができない。

実施例

以下、本発明の一実施例について図面を参照しながら説明する。

第1図は、本発明のICカード装置の構成を示した図である。

ICカード装置100において、補助電源140によってデータを保持できるRAM134はマスター鍵などの機密情報を格納し、RAM133はプログラムの実行時の作業領域等に使用される。

ICカード装置100は、入出力部120から得たコマンドを解析するプログラムあるいはシステムプログラムなどを格納するROM131あるいはEEPROM132と、これらプログラムを実行する中央演算部110とを有している。

第2図は、本発明のICカード装置を用いた受信装置の構成図である。ICカード装置230において、鍵格納部234は第1図のRAM134に相当し、制御部232および復号部233は第1図のROM131に相当し、これらの一連の流れを中央演算部110が制御し、処理がなされる。

受信装置200は放送データを受信し分割部210へ引き渡す。分割部210はこのデータを機密データ250と通信相手に伝えたい所望の伝送データ260とに分割する。この機密データ250はデスクランブルするための鍵パラメータであり暗号化されており、ICカード装置230に送信される。伝送データ260はデスクランブル部220に送信され、解読される。制御部232は入出力部231を通して得られた暗号化された鍵パラメータを復号部233に引き渡し、暗号化された鍵パラメータを復号することのできるマスター鍵が格納されている鍵格納部234を制御する。復号部233は制御部232からの暗号化された鍵パラメータと鍵格納部234から引き出したマ

スター鍵を用いて、伝送データ260をデスクランブルするための鍵パラメータを復号する。また入出力部231は復号部からの鍵パラメータ270を受信装置200のデスクランブル部220に送信する。デスクランブル部220はこの鍵パラメータ270をもとに伝送データをデスクランブルし最終出力する。

本発明のICカード装置230では、デスクランブル部220に用いる鍵を復号するための機密情報はRAM133に格納されており不正行為によってRAM133への電源供給が停止しするため、機密が守られる。

次に、不正行為等が行われた場合にRAMへの電源供給をストップする電源供給遮断手段について説明する。

第4図は本願発明の電源供給遮断手段の実施例を示したものである。

まず、第4図(a)において、410は中央演算部110、ROM131、EEPROM132、RAM133及びRAM134が搭載された1チ

ップのLSIである。このLSI410は、同図に示すように、ICカード装置100内部に埋め込まれており、外観からはLSI410の存在位置はわからないようになっている。140は第1図に示すものと同じものでRAM134へ電源を供給する補助電源である。420は電源供給遮断手段であり、補助電源140からLSI410内のRAM134に電源を供給するリード線で構成されている。同図に示すように、このリード線は補助電源140から出発して、ICカード装置100の内部を張り巡らすようにしたのち、電源供給先であるRAM134に接続されている。そして、第三者が複製あるいは暗号解析等の不正な目的で、LSI410を取り出そうとした場合は、このリード線を切断してしまい、RAM134への電源供給が断たれ、機密情報は消滅する。

なお、このリード線の引き回しの方法は、第4図(a)のようなものだけでなく、例えば第4図(b)に示すように、ICカード装置100の厚み方向に対して波状に引き回すことも容易に実

現できる。また、第4図(c)に示すようにICカード装置の内部を隙間なくきめ細かに網羅するように配線してもよい。このように配線の方法を複雑にすることで微細な不正行為に対しても電源を遮断することができる。

さらに、本実施例の受信装置200を用いた放送受信方式では、デスクランブル部220を公開することも可能であり、ICカード装置230の信頼性は本発明により著しく向上するので、契約者に限定した通信を確実に行うことができる。

このように本実施例によれば、ICカード装置100自体の安全性が著しく向上するので、このICカード装置100を用いた受信装置200においては、たとえ受信装置200のデスクランブル部220に入る復号化された鍵パラメータ270が盗聴されたとしても、この鍵パラメータ270は短い間隔で更新されていくため、衛生放送などの多量の情報をリアルタイムで処理する不正行為は不可能となる。

発明の効果

以上のように本発明によれば ICカード装置内の機密情報はRAMに格納されており不正行為によってRAMへの電源供給が遮断されるため機密情報が守られる。

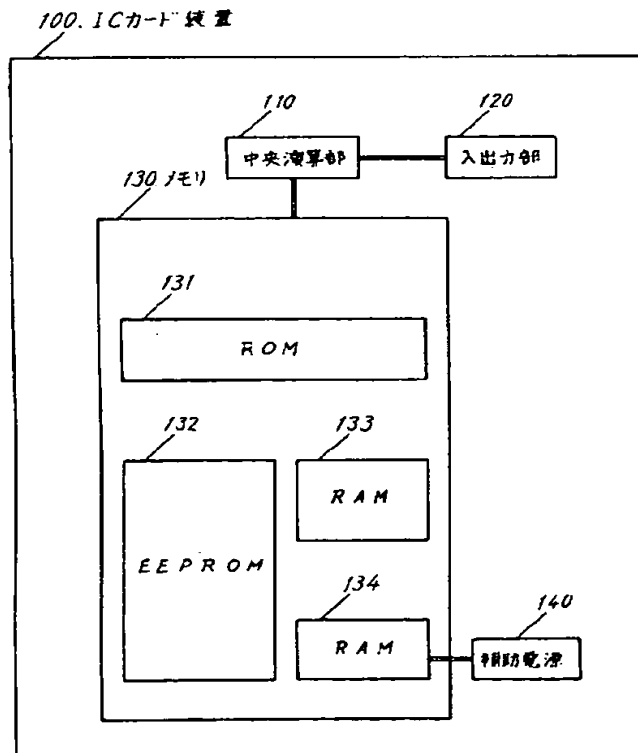
また このICカード装置を用いた受信装置においては デスクランブル部に入る鍵パラメータを盗聴したとしても 鍵パラメータは短い間隔で更新されていくため 多量の情報をリアルタイムで処理する不正行為は不可能となる。

4. 図面の簡単な説明

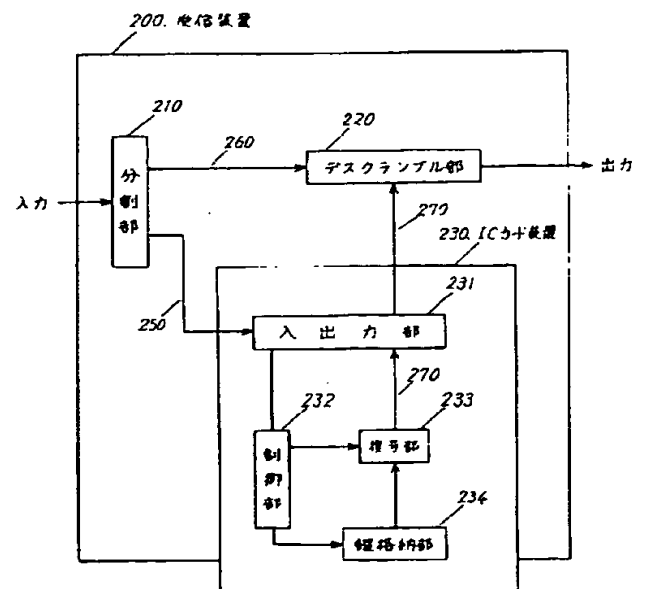
第1図は本発明のICカード装置の構成図 第2図は本発明のICカード装置を用いた受信装置の構成図 第3図は従来技術のICカード装置を用いた受信装置の構成図 第4図は本発明の電源供給遮断手段の一実施例を示す図である。

100・・・ICカード装置 110・・・中央演算部 120・・・入出力部
130(メモリ) 131・・・ROM 132・・・EEPROM 133・・・RAM 134・・・RAM 140・・・補助電源
200・・・受信装置 220・・・デスクランブル部 230(ICカード装置) 231・・・入出力部 232・・・制御部 233・・・符号部 234・・・格納部

第 1 図



第 2 図



第 4 図

第 3 図

